AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
21789 Windmill Loop NW, Poulsbo, WA 98370 and the person of Yusef Rahman Ali, more fully described in Attachment A

Case No. MJ20-5079

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
21789 Windmill Loop NW, Poulsbo, WA, and a person more fully described in Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2); and	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:

✓ See Affidavit of Special Agent Byron E. Garcia, Department of the Navy, NCIS, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or ☐ telephonically recorded.

Applicant's signature

BYRON E. GARCIA, Special Agent
Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 04/14/2020

Judge's signature

City and state: Tacoma, Washington

J. RICHARD CREATURA, United States Magistrate Judge
Printed name and title

USAO: 2020R00218

ATTACHMENT A

Items to be Searched

I. Description of the Property to be Searched (SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 21789 Windmill Loop NW, Poulsbo, WA 98370. The SUBJECT PREMISES is more fully described as the property containing a driveway that led from the northwest corner of Windmill Loop NW toward a two-story, three-bedroom single-family house approximately 1,792 square feet built in 2012 in an approximately 8,276 square foot lot. The front door and garage door were on the south side of the house, with the front door closer to the southwest corner and the garage door closer to the southeast corner. The number "21789" appeared vertically on the westernmost frame surrounding the garage door. The house had tan or light-brown siding, white or cream-colored accents, brownish shutters, and greyish-shingled roof. The south side of the house had two windows on the first floor and three windows on the second floor. A wooden fence surrounded a backyard and inset patio on the north side of the house.

The search is to include all rooms, attics, basements, and all other parts therein, any garages, outbuildings, or storage rooms, attached or detached, and any digital device(s) found therein. Specifically, this warrant authorizes law enforcement to seize and search any digital device law enforcement has probable cause to believe is owned by or to which the SUBJECT PERSON has access. For any other digital device, law enforcement may seize that device under this warrant but may not search it without approval from the Court.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

II. Description of the Person to be Searched (SUBJECT PERSON)

The person to be searched, YUSEF RAHMAN ALI, is an African American male born on XX/XX/1970.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

ATTACHMENT B

Items to be Seized

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON.

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of any associated email accounts, instant message accounts or other communications or digital storage such as cloud accounts.

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

8. Any non-digital recording devices and non-digital media capable of storing images and videos.

9. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above, including but not limited to computers, digital cameras, and smart phones;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

10. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

11. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

12. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

13. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

14. Evidence of times the digital device(s) was used;

15. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

SEARCH TECHNIQUES

1. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and log-ons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and will not include looking for personal documents and files that are unrelated to the crime.

2. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

3. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement determines that a particular digital device was not an instrumentality of the offenses listed above, that device shall be returned to the person from whom it was seized within sixty days of the date of the warrant, unless the government seeks and obtains permission from the Court for its retention.

4. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Byron E. Garcia, being duly sworn, state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Naval Criminal Investigative Service (NCIS) assigned to NCIS Resident Agency (NCISRA) Bangor, Washington, since December 2018. The Department of the Navy authorized me to conduct investigations for offenses enumerated in Title 18, United States Code, and Title 10, United States Code, also known as the Uniform Code of Military Justice (UCMJ), which affect the Department of the Navy, and specifically the United States Navy (USN) and United States Marine Corps (USMC). My duties include, but are not limited to, investigating crimes committed on or aboard naval installations, aircraft or vessels, committed by or against Navy or Marine Corps military personnel or civilian employees, or otherwise involving Department of the Navy assets, personnel, or facilities.

2. As part of my duties as an NCIS Special Agent, I investigate criminal violations relating to child exploitation and child pornography. I received training in the area of child pornography and child exploitation. I also participated in the execution of other search warrants involving investigations of child exploitation and/or child pornography offenses.

3. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: the premises at 21789 Windmill Loop NW, Poulsbo, Washington 98370 (the "SUBJECT PREMISES"), and the person of YUSEF RAHMAN ALI ("SUBJECT PERSON") more fully described in Attachment A to this Affidavit, for the property and items described in Attachment B to this Affidavit.

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

4. This application seeks a warrant to search the SUBJECT PREMISES and the SUBJECT PERSON, and seize the items listed in Attachment B, which is attached to this Affidavit and incorporated herein by reference, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

5. The facts set forth in this Affidavit are based on the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

6. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation. I have set forth only the facts I believe are relevant to the determination of probable cause to believe evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) will be found in the SUBJECT PREMISES and on the SUBJECT PERSON.

II. SUMMARY OF INVESTIGATION

7. On January 6, 2020, Special Agent Terrance POSTMA, Federal Bureau of Investigation (FBI) Poulsbo Resident Agency, notified NCISRA Bangor, Washington, the SUBJECT PERSON reportedly purchased and possessed child pornography from David DRAKE, the subject of a separate FBI investigation. I contacted the FBI's Birmingham Division, who provided copies of their reports, search warrant affidavit, and evidence obtained during their investigation of DRAKE for the advertisement, sale, and distribution of child pornography. My review of the copies of the aforementioned reports, affidavit, and evidence revealed the following information.

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

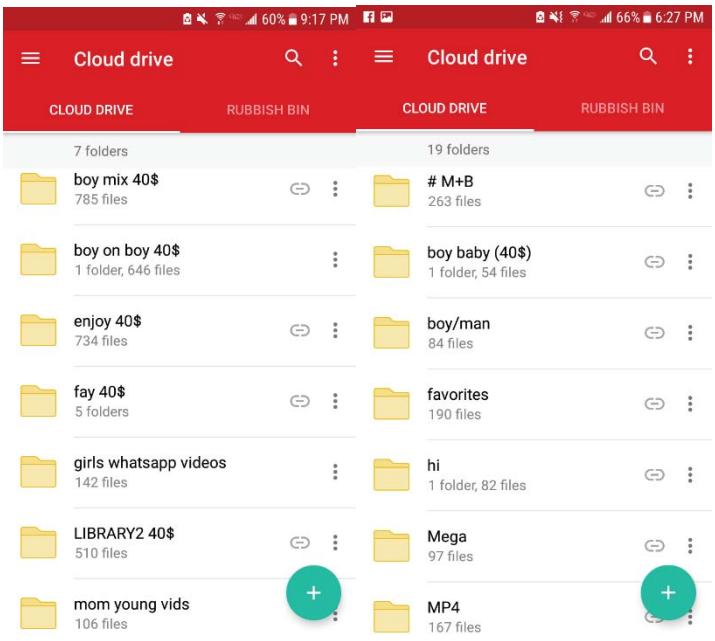
8. On August 13, 2018, Tumblr submitted a CyberTip report to the National Center for Missing and Exploited Children (NCMEC), CyberTipline Report: 38558313. Tumblr is a public blogging and publishing platform acquired by Yahoo circa 2013, and owned by Oath, Inc. The Tumblr service allows users to post multimedia to a public blog page for other users to view. The Tumblr report identified a user who uploaded approximately fifty (50) images and videos to Tumblr's servers, which depicted prepubescent and pubescent adolescents in various stages of undress and engaged in sexual acts. Tumblr reported the following subscriber information: User Name stopjealous22 and Profile/Public Universal Record Locator (URL) stopjealous22.tumblr.com.

9. On September 10, 2018, Yahoo, Inc. and Oath submitted a CyberTip report to NCMEC, CyberTipLine Report: 40005612, as a supplement to the previously filed CyberTipline Report: 38558313 from Tumblr. Yahoo, Inc. and Oath reported the following information regarding the email accounts: stopjealous22@yahoo.com and stopjealous22.tumblr.com: (1) the Yahoo account was created on July 12, 2018; (2) the phone number provided for the Yahoo account is "+1-2058070069," (3) this phone number was last verified on July 12, 2018, (4) the date of birth provided for the Yahoo Account was May 18, 1999, (5) the last successful login to the Yahoo account was on July 20, 2018, from Spectrum Business IP address 71.45.249.170, located in or around Birmingham, Alabama, (6) the user provided description for Tumblr blog stopjealous22.tumblr is "hmu on wickr sendmb6 30$."

10. On September 25, 2018, FBI Special Agents acting in an undercover capacity (UC) accessed the public online Tumblr blog, stopsleep8.tumblr.com. The blog advertised the sale of child pornography and contained images and videos that depicted prepubescent and pubescent boys in various stages of undress and engaged in sexual acts. The title of the blog stated: "Wickr sendmb6 to buy links." Wickr is an instant messaging app, which allows users to exchange end-to-end encrypted and content-expiring

messages, including photos, videos, and file attachments, and place end-to-end encrypted video conference calls. Wickr messages automatically delete after six (6) days.

11. On September 26, 2018, the UC contacted the user "sendmb6" via the Wickr application (app). The public avatar of "sendmb6" depicted the image of an adult male having sex with a boy who appeared to be under the age of twelve (12). "[S]endmb6" offered to sell the UC links to download videos of child pornography for either $30 or $40 depending on the link requested. The user "sendmb6" subsequently provided screenshots of a Mega Cloud Drive, which contained multiple folders that potentially contained child pornography. Examples of the folder names contained within the Mega Cloud Drive Account included "boy mix 40$," "boy on boy 40$," "and "boy baby (40$)."



12. On September 26, 2018, "sendmb6" offered to send the UC a sample video, and subsequently provided the UC with a Mega link to download a sample video. The sample video depicted a boy, who appeared under the age of twelve (12), performing oral sex on an adult male in the shower.

13. "[S]endmb6" requested payment via Cash App or Amazon gift card from the UC in order to complete the purchase of links. Cash App is a mobile payment service

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

developed by Square, Inc., which allows users to transfer money to one another using a mobile phone app. The UC presented "sendmb6" with an Amazon gift card worth $40 via the Wickr app. "[S]endmb6" subsequently provided the UC with a link to a Mega folder titled "boy on boy 40$." Mega is a cloud-based and file hosting service offered by Mega Limited, a New Zealand-based company. The Mega link contained a folder with approximately 641 videos. I reviewed copies of the aforementioned videos, which mostly depicted prepubescent boys under the age of twelve (12), in various stages of undress, engaged in sexual acts with other children and/or adult males.

14. The UC subsequently conducted two (2) additional controlled purchases from DRAKE. The third controlled purchase resulted in access to one of DRAKE's Dropbox accounts. I reviewed copies of the contents of the aforementioned Dropbox account, which contained approximately thirty (30) videos of prepubescent boys, most of whom appeared to be under the age of twelve (12), in various stages of undress, masturbating or engaged in sexual acts with other boys or adults.

15. The FBI served administrative subpoenas on Amazon.com Inc., Mega Limited, and Square, Inc. requesting information related to the aforementioned accounts associated with the user "sendmb6." The FBI reviewed the responses, and subsequently determined the user of "sendmb6" was DRAKE.

16. On May 30, 2019, the FBI interviewed DRAKE, who admitted the following: DRAKE advertised, sold, and distributed child pornography from his Tumblr page, and directed users to his "sendmb6" Wickr account to complete the sale of child pornography. According to DRAKE, "sendmb6" stood for "send man/boy." DRAKE subsequently sent these users a screenshot of his collection for the user to decide which folder the user wanted to purchase. DRAKE sold folders for $10 to $50, and divided each folder by the type and genre of child pornography it contained (e.g. man/boy, boy/boy). DRAKE accepted payment by Venmo, Cash App, or Amazon gift cards, and all payments to his Venmo, Cash App, and Amazon accounts directly resulted from his sale

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

of child pornography. DRAKE subsequently plead guilty to a federal indictment for the advertisement, sale, and possession of child pornography.

17. The FBI served an administrative subpoena to Square, Inc. regarding DRAKE's Cash App account, which identified several users who potentially purchased child pornography from DRAKE. According to Square, Inc. records, Cash App user "Carl" completed eight (8) transactions to DRAKE between August 26, 2018 and September 24, 2018.

18. The aforementioned administrative subpoena for Square, Inc. revealed the following account profile information further revealed the following account profile information for "Carl":

a. Customer Token: C_hxpgjaybf

b. Display Name (History): Yusef Ali

c. Date of Birth: May 1, 1970

d. Last Four of Social: 1447

e. Email (History): jusbreath80@gmail.com

f. Cashtag (History): baaq80

g. Address: 21789 Windmill Loop, Poulsbo, WA 98370

h. Payment Source History: Navy Federal Credit Union card, ZIP Code 98370 (link created at 26 August 2018)

i. Virtual Card Number: 4403931914051280

19. Square, Inc. indicated in their response the identifiers for sending or receiving peer-to-peer transactions included phone number, email, and Cashtag. Square, Inc. further advised they left the date of birth and Social Security Number (SSN) fields blank if the account had not met internal thresholds for identity verification. An Accurint search for "Yusef ALI" revealed the following information:

a. Name: Yusef R. Ali

b. Address: 21789 Windmill Loop NW, Poulsbo, WA 98370-9808

c. DOB: May 1, 1970

d. SSN: XXX-XX-1447

20. On January 6, 2020, I reviewed the Official Military Personnel File (OMPF) and database checks for the SUBJECT PERSON. The OMPF review revealed the SUBJECT PERSON was an Electronics Technician, Submarine, Navigation (ETV) in the United States Navy assigned to the Trident Refit Facility (TRF) in Naval Base Kitsap Bangor, Washington, located in the Western District of Washington. The full name, address, date of birth, and SSN in the SUBJECT PERSON's OMPF matched the subscriber information associated with "Carl" account and the address for the SUBJECT PREMISES. Database checks on Department of Defense Person Search (DPS) also confirmed the SUBJECT PERSON's full name, SSN, date of birth, and address matched the information associated with the "Carl" account and the address for the SUBJECT PREMISES. DPS checks further revealed the SUBJECT PERSON's email address was jus_breath80@yahoo.com, which matched the username of the Gmail address associated with the "Carl" account.

21. On January 9, 2020, I served a 2703(d) court order on Square, Inc. to disclose records and information associated with the "Carl" account from August 21, 2018, to present. On January 23, 2020, I received a response to the aforementioned 2703(d) court order, which included the Cash App account profile information for the "Carl" account, the eight (8) Cash App transactions between this account and DRAKE, and Internet Protocol (IP) logs from October 13, 2018, to October 22, 2019. The IP logs revealed the "Carl" account use accessed Cash App on fifty-two (52) dates and times using three (3) IP addresses. One of the IP addresses resolved to Verizon Wireless and two (2) IP addresses resolved to Comcast Cable Communications. The "Carl" account accessed Cash App using the Comcast IP address 24.22.228.102 (the "SUBJECT IP") for

the most recent forty-one (41) dates and times between October 22, 2018 to October 22, 2019.

22. On January 31, 2020, I served a 2703(d) court order requesting Comcast Corporation disclose records and information associated with the SUBJECT IP. On February 3, 2020, Comcast Corporation responded to the aforementioned 2703(d) court order, which revealed Comcast could not identify a subscriber account on the dates on or before 13 December 2018, but associated the SUBJECT IP on subsequent dates with the following subscriber:

a. Subscriber Name: [J.A]

b. Service Address: 21789 Windmill Loop NW, Poulsbo, WA 9837

c. Billing Address: 21789 Windmill Loop NW, Poulsbo, WA 98370

d. Telephone No.: (360) 689-4353

e. Type of Service: High Speed Internet Service

f. Start of Service: Unknown

g. Account Number: 8498360030804587

h. Account Status: Active

i. IP Assignment: Dynamically Assigned

j. MAC Address: 00:1d:d0:69:8e:e2

k. Email Users Ids: ladyjay1970@comcast.net

23. I further reviewed the Official Military Personnel File (OMPF) for the SUBJECT PERSON, which revealed he married J.A. on November 19, 2005, and they resided together in the SUBJECT PREMISES with their minor son as early as approximately August 21, 2012. A review of Kitsap County records for the SUBJECT PREMISES revealed calls for service from a Comcast alarm service from approximately 2012 to 2017.

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

24. As outlined above, multiple sources of information indicated the SUBJECT PERSON currently resides at the SUBJECT PREMISES; resided there on the dates of the eight (8) Cash App transactions between the SUBJECT PERSON and DRAKE; and resided there on the most recent dates the SUBJECT PERSON accessed Cash App, which the SUBJECT PERSON accessed via the SUBJECT IP. I know from my training and experience Cash App users rarely, if ever, share their accounts. As detailed above, the records and information for the "Carl" account matched the SUBJECT PERSON and the SUBJECT PREMISES. I therefore believe it likely the SUBJECT PERSON is the user of the "Carl" account, and he mostly recently and frequently accessed Cash App from the SUBJECT PREMISES using the SUBJECT IP. Given DRAKE admitted he only used Cash App to sell and distribute child pornography, there is probable cause to believe the SUBJECT PERSON received and possessed child pornography from DRAKE.

25. NCIS conducted records checks and surveillance of the SUBJECT PREMISES on multiple dates from January 7, 2020 to April 9, 2020, which revealed the SUBJECT PERSON resides at the SUBJECT PREMISES with his wife J.A. and their 13-year old son. The records checks and surveillance revealed no additional occupants in the SUBJECT PREMISES. The SUBJECT PREMISES are located on 21789 Windmill Loop NW, Poulsbo, Washington 98370, in the Western District of Washington.

III. TECHNICAL BACKGROUND

26. Based on my training and experience, when an individual communicates through the Internet, the individual leaves an IP address which identifies the individual user by account and ISP (as described above). When an individual is using the Internet, the individual's IP address is visible to administrators of websites they visit. Further, the individual's IP address is broadcast during most Internet file and information exchanges that occur.

27. Based on my training and experience, I know that most ISPs provide only one IP address for each residential subscription. I also know that individuals often use multiple digital devices within their home to access the Internet, including desktop and

laptop computers, tablets, and mobile phones. A device called a router is used to connect multiple digital devices to the Internet via the public IP address assigned (to the subscriber) by the ISP. A wireless router performs the functions of a router but also includes the functions of a wireless access point, allowing (wireless equipped) digital devices to connect to the Internet via radio waves, not cables. Based on my training and experience, today many residential Internet customers use a wireless router to create a computer network within their homes where users can simultaneously access the Internet (with the same public IP address) with multiple digital devices.

28. Based on my training and experience and information provided to me by computer forensic agents, I know that data can quickly and easily be transferred from one digital device to another digital device. Data can be transferred from computers or other digital devices to internal and/or external hard drives, tablets, mobile phones, and other mobile devices via a USB cable or other wired connection. Data can also be transferred between computers and digital devices by copying data to small, portable data storage devices including USB (often referred to as "thumb") drives, memory cards (Compact Flash, SD, microSD, etc.) and memory card readers, and optical discs (CDs/DVDs).

29. As outlined above, residential Internet users can simultaneously access the Internet in their homes with multiple digital devices. Also explained above is how data can quickly and easily be transferred from one digital device to another through the use of wired connections (hard drives, tablets, mobile phones, etc.) and portable storage devices (USB drives, memory cards, optical discs). Therefore, a user could access the Internet using their assigned public IP address, receive, transfer or download data, and then transfer that data to other digital devices, which may or may not have been connected to the Internet during the date and time of the specified transaction.

30. Based on my training and experience, I have learned that the computer's ability to store images and videos in digital form makes the computer itself an ideal repository for child pornography. The size of hard drives used in computers (and other digital devices) has grown tremendously within the last several years. Hard drives with

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

the capacity of four (4) terabytes (TB) are not uncommon. These drives can store thousands of images and videos at very high resolution.

31. Based on my training and experience, and information provided to me by other law enforcement officers, I know that people tend to use the same user names across multiple accounts and email services.

32. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

33. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

34. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera,

mobile phone, or tablet. These files can then be easily transferred from the mobile device to a computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

35. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

36. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another. Moreover, many media storage devices, including smartphones and thumb drives, can easily be concealed and carried on an individual's person and smartphones and/or mobile phones are also often carried on an individual's person.

37. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced

crimes that might be found at the SUBJECT PREMISES or on the SUBJECT PERSON, in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices, examples of which are enumerated in Attachment B to this Affidavit, an ideal repository for child pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

38. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides, and/or drawings or other visual media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any "hard copies" of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

their home or some other secure location. These individuals typically retain these "hard copies" of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual's residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

39. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices, including storage media, used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

40. Given the above-stated facts and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that the SUBJECT PERSON has a sexualized interest in children and depictions of children and that evidence of child pornography is likely to be found on digital media devices, including mobile and/or portable digital devices found at the SUBJECT PREMISES or on the SUBJECT PERSON.

41. Based on my training and experience, and that of computer forensic agents that I work and collaborate with on a daily basis, I know that every type and kind of information, data, record, sound or image can exist and be present as electronically stored information (ESI) on any of a variety of computers, computer systems, digital devices, and other electronic storage media. I also know that electronic evidence can be moved easily from one digital device to another. As a result, I believe that electronic evidence may be stored on any digital device present at the SUBJECT PREMISES or on the SUBJECT PERSON.

42. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data that is user-generated and found on a digital device. In other cases, these items may take

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

the form of other types of data - including in some cases data generated automatically by the devices themselves.

43. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe that if digital devices are found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is probable cause to believe that the items set forth in Attachment B will be stored in those digital devices for a number of reasons, including but not limited to the following:

a. Once created, ESI can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

IV. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

44. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby

trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

b. Volume of Evidence: The volume of data stored on many digital devices is typically so large that it is impossible to search for criminal evidence in a reasonable period of time during the execution of the physical search of a search site. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to two terabytes (2,000 gigabytes of data). Additionally, this data may be stored in a variety of formats or may be encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer).

c. Search Techniques: Searching the ESI for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

45. In this particular case, the government anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched, which will facilitate the search for evidence that does come within the items described in Attachment B. Further, the government anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and or suspected child pornography image files. Use of these tools will allow for the quick

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

identification of evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case.

46. Collectors of child pornography are known to transport their child pornography collections, which are often stored on mobile and/or portable digital media devices, with them throughout the day. In particular, I have consulted with law enforcement officers with experience investigating child exploitation related crimes, and have learned that collectors of child pornography have been found to transport their collections stored on mobile and/or portable devices 1) within pockets on their person, and 2) inside bags/backpacks that they carry, and/or 3) within compartments located inside their vehicle.

47. Because multiple people share the SUBJECT PREMISES and in order to protect the privacy of individuals who may not be suspects of criminal activity, executing agents will attempt to determine onsite which resident or residents own or have access to a given digital device. If executing agents can reasonably determine that the SUBJECT PERSON does not own or have access to a particular device, they will not seize or search that digital device.

48. However, if agents conducting the search nonetheless determine that it is probable that the things described in this warrant could be found on any computer(s) or digital device(s) in the residence, this application seeks permission to conduct an onsite search of those computers and digital devices as well, using forensic software, to determine if any child pornography is present. If, as a result of this onsite search, there is no child pornography present on those computers or digital devices, then they will not be searched further and will not be seized. However, agents will be authorized to seize any computer or digital device owned or used by SUBJECT PERSON for off-site forensic review, if an onsite forensic review is not possible or feasible.

49. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as

necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within sixty days of the date of the warrant, unless the government seeks and obtains permission from the Court for its retention.

50. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

V. GENUINE RISKS OF DESTRUCTION OF EVIDENCE

51. Any other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, for example, a consent search, could result in an unacceptable risk of the loss/destruction of the evidence sought. If agents pursued a consent-based interview of and/or a consent-based search of digital media belonging to the SUBJECT PERSON at the SUBJECT PREMISES, he could rightfully refuse to give consent and subsequently destroy all evidence of the crime before agents could return with a search warrant. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant.

VI. CONCLUSION

52. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located at the SUBJECT PREMISES or on the SUBJECT PERSON, as more fully described in Attachment A to this Affidavit, as well as on and in any digital

//

//

//

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

devices found therein. I therefore request that the court issue a warrant authorizing a search of the SUBJECT PREMISES and on the SUBJECT PERSON for the items more fully described in Attachment B.

BYRON E. GARCIA,
Affiant, Special Agent
Department of the Navy
Naval Criminal Investigative Service

Subscribed and sworn to before me this 14th day of April, 2020.

J. RICHARD CREATURA
United States Magistrate Judge

UNITED STATES ATTORNEY
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
(253) 428-3806

ATTACHMENT A

Items to be Searched

I. Description of the Property to be Searched (SUBJECT PREMISES)

The physical address of the SUBJECT PREMISES is 21789 Windmill Loop NW, Poulsbo, WA 98370. The SUBJECT PREMISES is more fully described as the property containing a driveway that led from the northwest corner of Windmill Loop NW toward a two-story, three-bedroom single-family house approximately 1,792 square feet built in 2012 in an approximately 8,276 square foot lot. The front door and garage door were on the south side of the house, with the front door closer to the southwest corner and the garage door closer to the southeast corner. The number "21789" appeared vertically on the westernmost frame surrounding the garage door. The house had tan or light-brown siding, white or cream-colored accents, brownish shutters, and greyish-shingled roof. The south side of the house had two windows on the first floor and three windows on the second floor. A wooden fence surrounded a backyard and inset patio on the north side of the house.

The search is to include all rooms, attics, basements, and all other parts therein, any garages, outbuildings, or storage rooms, attached or detached, and any digital device(s) found therein. Specifically, this warrant authorizes law enforcement to seize and search any digital device law enforcement has probable cause to believe is owned by or to which the SUBJECT PERSON has access. ~~For any other digital device, law enforcement may seize that device under this warrant but may not search it without approval from the Court.~~ JRC

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

II. Description of the Person to be Searched (SUBJECT PERSON)

The person to be searched, YUSEF RAHMAN ALI, is an African American male born on XX/XX/1970.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

ATTACHMENT B

Items to be Seized

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, smart cards, thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found at the SUBJECT PREMISES or on the SUBJECT PERSON.

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of any associated email accounts, instant message accounts or other communications or digital storage such as cloud accounts.

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all address books, names, lists of names, telephone numbers, and addresses of minors;

7. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

8. Any non-digital recording devices and non-digital media capable of storing images and videos.

9. Digital devices and/or their components, which include, but are not limited to:

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above, including but not limited to computers, digital cameras, and smart phones;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

10. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

11. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

12. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

13. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

14. Evidence of times the digital device(s) was used;

15. Any other ESI from the digital device(s) necessary to understand how the digital device was used, the purpose of its use, who used it, and when.

SEARCH TECHNIQUES

1. In this particular case, and in order to protect the third party privacy of innocent individuals residing in the residence, the following are search techniques that will be applied:

i. Device use and ownership will be determined through interviews, if possible, and through the identification of user account(s), associated account names, and log-ons associated with the device. Determination of whether a password is used to lock a user's profile on the device(s) will assist in knowing who had access to the device or whether the password prevented access.

ii. Use of hash value library searches.

iii. Use of keyword searches, i.e., utilizing key words that are known to be associated with the sharing of child pornography.

iv. Identification of non-default programs that are commonly known to be used for the exchange and viewing of child pornography, such as, eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

v. Looking for file names indicative of child pornography, such as, PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the undercover download of child pornography.

vi. Viewing of image files and video files.

vii. As indicated above, the search will be limited to evidence of child pornography and will not include looking for personal documents and files that are unrelated to the crime.

2. These search techniques may not all be required or used in a particular order for the identification of digital devices containing items set forth in Attachment B to this Affidavit. However, these search techniques will be used systematically in an effort to protect the privacy of third parties. Use of these tools will allow for the quick identification of items authorized to be seized pursuant to Attachment B to this Affidavit, and will also assist in the early exclusion of digital devices and/or files which do not fall within the scope of items authorized to be seized pursuant to Attachment B to this Affidavit.

3. In accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. Upon securing the search site, the search team will conduct an initial review of any digital devices/systems to determine whether the ESI contained therein can be searched and/or duplicated on site in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. If, based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site search, or to make an on-site copy of the ESI within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices will be seized and transported to an appropriate law enforcement laboratory for review and to be forensically copied ("imaged"), as appropriate.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

c. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of any digital device that is found to contain data or items that fall within the scope of Attachment B of this Affidavit. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

d. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.

e. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement determines that a particular digital device was not an instrumentality of the offenses listed above, that device shall be returned to the person from whom it was seized within sixty days of the date of the warrant, unless the government seeks and obtains permission from the Court for its retention.

4. In order to search for ESI that falls within the list of items to be seized pursuant to Attachment B to this Affidavit, law enforcement personnel will seize and search the following items (heretofore and hereinafter referred to as "digital devices"), subject to the procedures set forth above:

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800

a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;

b. Any digital device used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, cameras, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, flash drives, thumb drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the device hardware, or ESI to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device, or ESI; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or ESI.

The seizure of digital devices and/or their components as set forth herein is specifically authorized by this search warrant, not only to the extent that such digital devices constitute instrumentalities of the criminal activity described above, but also for the purpose of the conducting off-site examinations of their contents for evidence, instrumentalities, or fruits of the aforementioned crimes.

UNITED STATES ATTORNEY
1201 Pacific Ave., Suite 400
Tacoma, Washington 98402
(253) 428-3800